

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

Purpose

As school systems increasingly seek to improve curricular and classroom experiences for learners, Vendor access to certain student data has become necessary. It has become equally important to ensure that vendors employ commercially reasonable methods to safeguard student data privacy. Accordingly, these STUDENT DATA PRIVACY REQUIREMENTS apply to all vendors of software, applications, or services that require access to the Personally Identifiable Information (“PII” as further defined herein) of Essex County Public Schools’ (ECPS) students. ECPS hereinafter is referred to as “School System” or “Licensee.”

These requirements will be published on the ECPS Web site.

These STUDENT DATA PRIVACY REQUIREMENTS (hereinafter referred to as “Privacy Requirements”), represent standard terms and conditions for all vendors who require access to student data to provide services to the School System. In the event of a conflict between these Privacy Requirements and any license agreement with the Vendor, these Privacy Requirements control.

Vendor’s Certification

By agreeing to these Privacy Requirements, the Vendor certifies, under the penalties of perjury, that Vendor complies with all federal and state laws, regulations and rules as such laws may apply to the receipt, storing, maintenance or access to personal information, including without limitation, all standards for the protection of personal information of residents of the Commonwealth of Virginia and maintaining safeguards for personal information. Vendor hereby further certifies under penalties of perjury that it has a written comprehensive information security program and that Vendor shall fully comply with the provisions of the federal Family Educational Rights and Privacy Act, 20 U.S.C. §1232g and regulations promulgated thereunder and its Commonwealth of Virginia counterparts. Vendor further agrees to comply with all of the mandates, protocols and practices established by these Privacy Requirements.

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

1. DEFINITIONS

“ANONYMIZED DATA” means a method of information sanitization whose intent is privacy protection. It is the process of either irreversibly encrypting or removing personally identifiable information (PII) from data sets, so that the persons named, described or otherwise identified in such data sets remain anonymous and cannot be re-identified.

“CLOUD STORAGE” means any remote server on which data or applications are housed or maintained. For the purposes of these Privacy Requirements, cloud storage includes private, public, community, hybrid and partner clouds.

“CLEAR” means a method of sanitization that applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

“DE-IDENTIFIED SCHOOL SYSTEM DATA” means data files that have all direct and indirect personal identifiers removed, including any data that could be analyzed and linked to other data to identify the student or the student’s family members, including without limitation parents/guardians. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location data, and federal, state and/or local school identification numbers.

“END USER” means the individuals authorized by the School System to access and use the services provided by the Vendor under the Privacy Requirements.

“LICENSEE” OR “SCHOOL SYSTEM” means Essex County Public Schools.

“LICENSEE DATA” OR “SCHOOL SYSTEM DATA” means all confidential student records or confidential student record information, however documented, that contains personally identifiable student records and any other non-public student information, including but not limited to student data, metadata and user content.

“MINING SCHOOL SYSTEM DATA” means to search through, access or extract School System data, metadata or information, which is not necessary to accomplish the purpose(s) of the Privacy Requirements.

“MOBILE DEVICE” means laptop computers, tablets, smart phones and any other mobile computing devices.

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

“PERSONALLY IDENTIFIABLE INFORMATION” OR “PII” includes but is not limited to: personal identifiers such as name, address, phone number, dates of birth, Social Security number, and student or personnel identification number. Students' personally identifiable information and/or any successor laws or regulations of the Commonwealth of Virginia; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act (“FERPA”), 20 USC §1232g; “medical information” or “medical records” as defined in the Code of Virginia §32.1-116.1:1; “protected health information” as the term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; “nonpublic personal information” as the term is defined in the Gramm-Leach-Bailey Financial Modernization Act of 1999, 15 USC §6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license numbers; and state-or federal-identification numbers such as passport, visa or state identity card numbers; and “covered information”.

“PORTABLE STORAGE MEDIUM” means portable memory devices, including jump or thumb drives, portable hard drives, tape backup media and cloud storage.

“SECURELY CLEARED” means taking action that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-88 guidelines relevant to data categorized as high security, confidential student records or confidential student record information that contains personally identifiable information, personally identifiable student records, and any other non-public information, including but not limited to student data, metadata and user content.

“SECURITY BREACH” means an event in which School System Data is exposed to unauthorized disclosure, access, alteration or use.

“SYSTEMS” means any of Vendor's computer system, network or software that accesses, maintains, stores or transmits School System Data, including computer systems or networks operated by Vendor, Vendor Personnel, Vendor contractors or subcontractors.

“STUDENT DATA” means any data about or related to a student, including information about a student's parent or legal guardian.

“VENDOR PERSONNEL” means any employee, officer, director, agent, affiliate, contractor or subcontractor of Vendor.

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

2. ACCESS, CONTROL AND AUTHORIZATION

2.1. Vendor agrees to protect and maintain the security of Licensee Data and PII with commercially reasonable security measures commensurate with the sensitivity of such PII. Without prior written permission, no Licensee Data and PII may be disclosed, sold, assigned, leased, shared or otherwise distributed to third parties by the other party or commercially exploited by or on behalf of the other party, or its employees or agents except when required by the Virginia Freedom of Information Act (FOIA).

2.2. Vendor shall not authorize access to Licensee Data and/or PII to any of its agents, affiliates, contractors and subcontractors, or to any auditor, unless such agent, affiliate, contractor, subcontractor or auditor has entered into a written confidentiality agreement with Vendor and Licensee agreeing to protect the confidentiality and security of such student PII. Such written confidentiality agreement shall be made available for inspection, upon demand, to the Licensee.

2.3. Vendor shall not permit unauthorized access to Licensee's student PII to any individual or entity at any time.

2.4. Vendor shall not provide any School System Data or PII or any portion thereof to any person, party or organization ineligible to receive student records and/or student record data and information protected by FERPA, federal regulation, Virginia law, Virginia regulation or so prohibited from receiving the School System Data or PII or any portion thereof.

2.5. Vendor understands and agrees that the purpose and contemplated use of the data and information disclosed by the Licensee is solely to provide the educational services for, or on behalf of the Licensee described herein. The Vendor shall be designated a "school official" according to FERPA, as an organization to which the Licensee has outsourced institutional services or functions for which the Licensee would otherwise utilize its own employees. The Vendor acknowledges that it is under the direct control of the Licensee for the purposes of use and maintenance of education records disclosed pursuant to this Agreement, and the Vendor agrees to comply with the applicable provisions of FERPA in order to safeguard the confidentiality of student information. 20 U.S.C. § 1232g(b)(1)(F) and 34 CFR § 99.31(a)(1)(i)(B).

3. PRIVACY COMPLIANCE

3.1. Vendor agrees to protect and maintain the privacy of Licensee Data and PII with commercially reasonable measures commensurate with the sensitivity of such Licensee Data.

3.2. Vendor certifies that it has implemented policies and procedures to protect against reasonably foreseeable unauthorized access to, or disclosure of, Licensee Data or PII, and to prevent other reasonably foreseeable events that may result in substantial harm to Licensee or any individual student identified in such PII.

3.3. Vendor shall not permit School System Data or PII to be maintained or stored on any Mobile Device or Portable Storage Medium unless such is being used in connection with Vendor's backup and recovery procedures and/or encrypted. Vendor will ensure that School System Data is encrypted and that all device/medium will be scanned at the completion of any contract or service agreement and/or research study or project to ensure that no School System Data, PII, personal

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

information and/or student record information is stored on such electronic devices/medium. Furthermore, Vendor will have in place a service that will allow vendor to wipe the hard drive on any stolen laptop or mobile electronic device remotely and have a protocol in place to ensure compliant use by employees.

3.4. Vendor shall not, **without the express prior written consent of School System:**

- (a) Maintain or store School System Data or PII outside of the United States,
- (b) Transmit Licensee's Data or PII to any contractors or subcontractors located outside of the United States,
- (c) Distribute, repurpose or share School System Data or PII with any Vendor Systems not used for providing services to the School System,
- (d) Use PII or any portion thereof to inform, influence or guide marketing or advertising efforts, or to develop a profile of a student or group of students for any commercial purpose [or for any other purposes],
- (e) Use PII or any portion thereof to develop commercial products or services,
- (f) Use any PII for any other purpose other than in connection with the services provided to the School System,
- (g) Engage in targeted advertising, as defined by the Code of Virginia § 22.1-289.01. School service providers; school-affiliated entities; student personal information.
- (h) Use any de-identified School System Data for internal product development and improvement and/or research, however, only after data fields have been defined.
- (i) Attempt to re-identify de-identified School System Data, or
- (j) Transfer de-identified School System Data to any party unless that party agrees in writing not to attempt re-identification.

3.5. Except as specifically set forth in these Privacy Requirements, or as required by federal or state law, Vendor shall not allow unauthorized access to, or permit the release of, School System Data or PII to any individual or entity except as follows:

- (a) To the Vendor's contractors or subcontractors that provide services related to the support, maintenance, and security of Vendor's software products or online services, provided, however, that such contractors or subcontractors agree to be subject to the terms and conditions of these privacy requirements.

4. BREACH PLANNING, NOTIFICATION, AND REMEDIATION

4.1. Vendor certifies that it has implemented policies and procedures addressing a potential Security Breach and that it possesses an up to date SecurityBreach response plan. Such plan shall be made available, upon request, to the School System.

4.2. Vendor shall comply with all applicable federal and state laws that require notification to individuals, entities, state agencies, or federal agencies in the event of a Security Breach.

Essex County Public Schools

STUDENT DATA PRIVACY REQUIREMENTS

Page 5 of 14

V1 – Updated: 5/21/2019

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

4.3. Security Breach

- (a) In the event of a circumstance that resulted in unauthorized access to or disclosure or use of School System Data, Vendor will notify the Chief Technology Officer or Superintendent of the School System directly confirming their knowledge of the event within three calendar days, Vendor will fully investigate the incident and cooperate fully with the School System's investigation of and response to the incident as soon as practicable, and/or is permitted by law enforcement agencies. Except as otherwise required by law, Vendor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the School System.
- (b) **Liability.** In addition to any other remedies available to the School System, at law or in equity, Vendor will reimburse the School System in full for all documented cost incurred by the School System in investigating and remediating any Security Breach caused in whole or in part by Vendor or Vendor's subcontractors, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed against the School System as a result of the Security Breach. Vendor will not have any liability to the extent the Security Breach is not caused by Vendor or Vendor's subcontractors

4.4. In the event of a Security Breach, Vendor shall:

- (A) Assume responsibility for providing the notification required under the applicable federal and/or state law(s) to School System only;
- (B) Hold harmless and indemnify School System and any of School System's school board members and employees, against all losses, damages, costs or expenses ("Losses") that school system may incur to the extent that such Losses arise directly from any willful or negligent acts or omissions of the Vendor in the handling of School System Data and/or PII which results in an event requiring notification of a Security Breach under applicable federal or state law. Vendor will not have any liability to the extent the Loss is caused by agents, contractors or representatives of School System or any of the School System's employees or is not caused by Vendor or Vendor's subcontractors. The foregoing indemnification obligations are subject to the School System promptly notifying the Vendor in writing of such claim, provided that the Vendor shall be relieved of its obligations under this only to the extent it is prejudiced by any delay in notification. The Vendor shall have sole control over the defense and settlement of such claim, provided that any settlement containing any binding obligations, admissions, or liability of the School System shall require School System's prior written consent.

School System shall have the right at its own expense, to participate in such litigation and settlement discussions without unreasonably interfering with

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

Vendor's ability to perform its obligations under this Section. School System shall provide all information and assistance reasonably requested by the Vendor at Vendor's expense;

- (C) Use commercially reasonable efforts to mitigate any negative consequences caused to School System or to a student as the result of such Security Breach; and
- (D) Use commercially reasonable efforts to implement procedures to prevent the recurrence of an event similar to such Security Breach.

5. INFORMATION STORAGE, RETENTION, AND DISPOSITION

5.1. Vendor certifies that it has implemented policies and procedures to address the storage, retention, and disposition of all School System Data prior to contract signing.

5.2. Vendor shall perform regular backups of School System Data and shall retain backup copies of such School System Data for such period of time as may be required by federal or state law, or by the School System.

5.3. Vendor shall maintain and store backup copies of School System Data at multiple secure storage facilities located within the United States and provide status reports upon request to the School System.

5.4. Except as specifically set forth in these Privacy Requirements, or as required by federal or state law, Vendor shall only retain the School System Data that is necessary to provide the contracted services set forth under any Agreement with the School System, shall Clear, or return to School System, any School System Data that is no longer necessary to provide such services as defined yearly and/or based on a schedule to be agreed upon between Vendor and the School System.

5.5. Vendor shall maintain and store the audit logs of its systems on a secured server location. Vendor shall restrict access to such audit logs to prevent tampering with or altering of the audit data. Vendor shall retain and provide audit logs for a minimum of 90 days to allow the School System or the Vendor to review the audit data for indications of a Security Breach.

6. DISPOSAL OF INFORMATION UPON TERMINATION OF AGREEMENT OR VENDOR'S CESSATION OF OPERATIONS

6.1. Except as specifically set forth in these Privacy Requirements, or as required by federal or state law or regulation, upon termination or expiration of the Agreement to provide services or products to the School System, Vendor shall:

- (a) Return all School System Data to the School System, pursuant to the terms and conditions of any agreements between Vendor and School System (the "Agreement");
- (b) Erase, Clear, or render unreadable all School System Data in a manner that prevents its physical reconstruction using commonly available file restoration utilities;
- (c) Certify in writing, by delivering to the School System the certificate attached hereto,

Essex County Public Schools

STUDENT DATA PRIVACY REQUIREMENTS

Page 7 of 14

V1 – Updated: 5/21/2019

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

that the actions set forth in this section have been completed on or before the agreed-upon deadlines set forth in any agreement entered into between the Vendor and the School System;

- (d) Ensure that any transfer/migration of School System Data uses facilities and methods that are compatible with the relevant systems of the School System or its designated third party; and
- (e) To the extent technologically possible, ensure that the School System will have access to School System Data during any transfer of operations.

6.2. Upon cessation of its operations or dissolution of its business operations, Vendor shall within 15 days or as soon thereafter as reasonably feasible under the circumstances, Clear all School System Data be it digital, archival or physical form, including without limitation any copies of the School System Data or any files that may reside in system backups, temporary files or other storage, media and School System data that are otherwise still in Vendor's possession and/or in the possession of any of the Vendor's subcontractors, or agents to which the Vendor may have transferred School System Data or any portion thereof, in a manner consistent with technology best practices and industry standards for secure data disposal methods. Vendor shall provide ECPS with written certification of clearance of all school system data within 30 days.

7. SURVIVAL

The confidentiality obligations set forth in these Privacy Requirements shall survive the termination of any agreement between the Vendor and the School System for as long as the PII and School System Data remain confidential.

8. DATA AUTHENTICITY AND INTEGRITY

Vendor will take reasonable measures, including maintaining audit trails, to protect School System Data against deterioration or degradation of data quality and authenticity.

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

9. RESPONSE TO LEGAL ORDERS, DEMAND OR REQUESTS FOR DATA

9.1. Except as otherwise expressly prohibited by law, Vendor will:

- (a) as soon as practicable, notify the School System of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking School System Data;
- (b) Consult with the School System regarding its response; cooperate with the School System's reasonable requests in connection with efforts by the School System to intervene and quash or modify the legal order, demand or request; and
- (c) as soon as practicable, upon the School System's request, provide the School System with a copy of its response.

9.2. If the School System receives a subpoena, warrant, or other legal order, demand or request seeking School System Data maintained by Vendor, the School System will promptly provide a copy of the application to Vendor. Vendor will promptly supply the School System with copies of records or information required in order for the School System to respond and will cooperate with the School System's requests in connection with its response.

9.3. Upon receipt of a litigation hold request, Vendor will preserve all documents and School System Data as identified in such request, and suspend any operations that involve overwriting, or potential destruction of documentation arising from such litigation hold.

10. GOVERNING LAW

These Privacy Requirements and all related requirements shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia. Any action to enforce the School System's rights and remedies shall be initiated in the Circuit Court for the County of Essex, VA.

11. SCHOOL SYSTEM'S RIGHT TO PROTECT PII OR SCHOOL SYSTEM DATA

In the event of a claim, suit, action, or proceeding against Vendor in which Vendor cannot, or will not, defend itself, and there is a reasonable likelihood that School System Data or PII may be disclosed to an unauthorized party in connection with such claim, suit, action, or proceeding; and Vendor provides notice to Licensee that it cannot, or will not, defend itself in such claim, suit, action, or proceeding, Vendor grants Licensee the right, but not the obligation, to join in such claim, suit, action, or proceeding to defend against the disclosure of School System Data or PII.

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

12. SECTION HEADINGS

The headings of sections in the Privacy Requirements are for reference only and shall not affect the meaning of the Privacy Requirements.

13. INTELLECTUAL PROPERTY RIGHTS/DISCLOSURE/OWNERSHIP

13.1. Unless expressly agreed to the contrary in writing, all School System Data or PII prepared by Vendor (or its subcontractors) for the School System will not be disclosed to any other person or entity.

13.2. Vendor warrants to the School System that the School System will own all rights, title and interest in any and all intellectual property created in the performance of the Privacy Requirements and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. Vendor agrees to assign and hereby assigns all rights, title, and interest in any and all School System- created intellectual property created in the performance of the Privacy Requirements to the School System and will execute any future assignments or other documents needed for the School System to document, register, or otherwise perfect such rights. Notwithstanding the foregoing, vendor retains all right, title and interest in and to its software, documentation, training and implementation materials and other materials provided in connection with vendor's services (collectively, "vendor ip"). Vendor grants to the school system a personal, nonexclusive license to use the vendor ip for its own non-commercial, incidental use as set forth in the end user license agreement accompanying such software and as contemplated herein. All data of the School System remains the property of the School System.

13.3. It is understood and agreed that ECPS is the exclusive Owner of School System Data and that at no point in time does or will the Vendor become the Owner of any School System Data, PII or School System files, and that should the Vendor be subject to dissolution or insolvency, School System files will not be considered an asset or property of the Vendor. Personally identifiable information from student records may only be re-disclosed by Vendor to a third-party with the prior written approval of the School System, in accordance with this Agreement or in compliance with FERPA and its regulations. The School System reserves the right to demand the prompt return of any School System Data and PII at any time and for any reason whatsoever.

14. DATA PRIVACY

14.1. Vendor will use School System Data only for the purpose of fulfilling its duties under the Privacy Requirements and except as authorized by the Privacy Requirements will not share such data, including anonymized data, with or disclose it to any third party without the prior written consent of the School System. The vendor further agrees not to disclose any such data to third party service providers used in connection with providing services to the School System, unless such third-party service providers are under this written obligation of confidentiality with respect to School System Data and use school system data solely to provide services to the School System and to vendor.

14.2. School System Data will not be stored outside the United States without prior written consent

Essex County Public Schools

STUDENT DATA PRIVACY REQUIREMENTS

Page 10 of 14

V1 – Updated: 5/21/2019

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

from the School System.

14.3. Vendor will provide access to School System Data, including anonymized only to its employees and subcontractors who need to access the data to fulfill Vendor obligations under the Privacy Requirements. Vendor will ensure that employees and subcontractors who perform work under the Privacy Requirements have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of the Privacy Requirements. If Vendor will have access to “education records” or “student records” of the School System’s students as defined under the Family Educational Rights and Privacy Act (FERPA), the Vendor acknowledges that for the purposes of the Privacy Requirements, it will be designated as a “school official” with “legitimate educational interests” in the School System education records, as those terms have been defined under FERPA and its implementing regulations, and the Vendor agrees to abide by the FERPA limitations as well as those limitations established by state law and regulation, and requirements imposed on school officials. Vendor will use the education records only for the purpose of fulfilling its duties under the Privacy Requirements for School System’s benefit and will not share such data with or disclose it to any third party except as provided for in the Privacy Requirements, required by law, or authorized in writing by the School System.

14.4. Vendor will not use School System Data (including metadata) for advertising or marketing purposes.

14.5. Vendor agrees to assist School System in maintaining the privacy of School System’s Data as may be required by State and Federal law, including but not limited to the Protection of Pupil Rights Amendment (PPRA), the Children’s Online Privacy Protection Act (COPPA), and their Commonwealth of Virginia counterparts, including, but not limited to the Code of Virginia § 22.1-289.01 and § 22.1-287.02.

14.6. Vendor is prohibited from mining School System Data for any purposes other than those agreed to by the Parties.

15. DATA SECURITY

Vendor will store and process School System Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration and use. Such measures will be no less protective than those used to secure Vendor’s own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Vendor warrants that all electronic School System Data will be encrypted in transmission (using a School System-approved encryption protocol that adheres to industry best practices).

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

16. AUDITS

16.1. The School System reserves the right in its sole discretion to perform audits of Vendor no more than once per twelve (12) month period at the School System's expense to ensure compliance with the terms of the Privacy Requirements. The Vendor shall reasonably cooperate in the performance of such audits. This provision applies to all agreements under which the Vendor must create, obtain, transmit, use, maintain, process or dispose of School System Data.

16.2. If the Vendor must under the Privacy Requirements create, obtain, transmit, use, maintain, process or dispose of the subset of School System Data known as Personally Identifiable Information or financial or business data which has been identified to the Vendor as having the potential to affect the accuracy of the School System's financial statements, Vendor will at its expense conduct or have conducted at least annually:

- (a) American Institute of CPAs Service Organization Controls (SOC) Type II audit, or other security audit with audit objectives deemed sufficient by the School System, which attests the Vendor's security policies, procedures and controls;
- (b) vulnerability scan, performed by a scanner approved by the School System, of Vendor's electronic systems and facilities that are used in any way to deliver electronic services under the Privacy Requirements; and
- (c) formal penetration test, performed by a process and qualified personnel approved by the School System, of Vendor's electronic systems and facilities that are used in any way to deliver electronic services under the Privacy Requirements.

16.3. The Vendor will provide the School System upon request an executive summary of the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under the Privacy Requirements. The School System may require the Vendor to perform additional audits and tests, the results of which will be provided promptly to the School System.

17. COMPLIANCE

17.1. Vendor will comply with all applicable laws and industry standards in performing services under the Privacy Requirements. Any Vendor personnel visiting the School System's facilities will comply with all applicable School System policies regarding access to, use of, and conduct within such facilities. The School System will provide copies of such policies to Vendor upon request.

17.2. Vendor warrants that any subcontractors used by Vendor to fulfill its obligations under the Privacy Requirements will be subject to and will be directed to comply with each and every term of the Privacy Requirements.

17.3. Vendor warrants that the service it will provide to the School System is fully compliant with and will enable the School System to be compliant with relevant requirements of all laws

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

applicable to Vendor, including but not limited to: the Children’s Online Privacy Protection Act (COPPA); Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Protection of Pupil Rights Amendment (PPRA); Americans with Disabilities Act (ADA), and Federal Export Administration Regulations.

18. CONFLICT

If there is any conflict or potential conflict between these Privacy Requirements and the terms of any other agreements between the parties, these Privacy Requirements shall control.

19. SURVIVAL

The Vendor’s obligations under Section Six (6) shall survive termination of these Privacy Requirements until all School System Data has been returned or Securely Cleared.

IN WITNESS WHEREOF, this Contract has been executed as of the date of the last party to sign below (“Effective Date”). If signed in counterparts, then each shall be considered an original thereof.

SCHOOLS

VENDOR

X: _____

X: _____

By: _____

By: _____

Title: Director of Technology

Title: _____

Date: Wednesday, June 5, 2019

Date: _____

ESSEX COUNTY PUBLIC SCHOOLS

Data Security and Privacy Agreement - DSPA

Attachment 1

Certification of Destruction/Return of School System Information

I/We, _____, as the authorized representative(s) of the Vendor _____ do hereby acknowledge and certify under penalty of perjury that [check one]:

_____ (a) the private and confidential student information provided by the School System as part of the Data Security and Privacy Agreement in accordance with federal and state law was destroyed.

_____ (b) the private and confidential student information provided by the School System as part of the Data Security and Privacy Agreement in accordance with federal and state law has been returned.

Print Name: _____ Date: _____

Title: _____

Vendor/Agency: _____

Signature: _____